Cyberstalking on Social Networking Sites and the Criminal Offences under Thai Law
การตามรังควานบนเว็บไซต์เครือข่ายสังคมและความผิดอาญาตามกฎหมายไทย

ดร. จอมพล พิทักษ์สันตโยธิน
อาจารย์ประจำคณะนิติศาสตร์
มหาวิทยาลัยหอการค้าไทย

Dr. Jompon Pitaksantayothin
Lecturer, School of Law
University of the Thai Chamber of Commerce
E-mail: jompom__pit@utcc.ac.th; tikpik@hotmail.com

บทคัดย่อ

การตามรังควานบนอินเทอร์เน็ตเป็นรูปแบบหนึ่งของการคุกคามที่เกิดขึ้นในพื้นที่ไซเบอร์ (Cyberspace) ก่อให้เกิดความเสียหายโดยเฉพาะบาดแผลทางจิตใจแก่ผู้ตกเป็นเหยื่อ เหยื่อบางรายอาจเกิดความกังวล ความกลัว จนไปถึงความคิดที่จะฆ่าตัวตาย การที่ปัจจุบันเว็บไซต์เครือข่ายสังคมเป็นที่นิยมแพร่หลาย ผู้ตามรังควานบางรายจึงใช้เว็บไซต์เครือข่ายสังคมเป็นเครื่องมือในการคุกคามเหยื่อ ตลอดช่วงเวลาไม่กี่ปีที่ผ่านมา ได้มีการรายงานเกี่ยวกับการตามรังควานบนเว็บไซต์เครือข่ายสังคมที่เกิดขึ้นทั้งในประเทศไทยและต่างประเทศหลายกรณีด้วยกัน

บทความนี้มุ่งที่จะศึกษาลักษณะของการตามรังควานบนเว็บไซต์เครือข่ายสังคมที่เกิดขึ้น และวิเคราะห์ว่าประเทศไทยมีกฎหมายใดที่จะสามารถนำมาปรับใช้ เพื่อเอาผิดทางอาญากับผู้ตามรังควานบนเว็บไซต์เครือข่ายสังคมได้บ้างและอย่างไร จากการศึกษา พบว่า ความผิดฐานข่มขืนใจผู้อื่น (มาตรา 309) การหมิ่นประมาท (มาตรา 326 และ มาตรา 328) และ การทำให้ผู้อื่นเกิดความกลัว (มาตรา 392) แห่งประมวลกฎหมายอาญา พ.ศ. 2499 และ ความผิดฐานข้อมูลคอมพิวเตอร์ปลอมหรือเท็จ (มาตรา 14(1)) และการเผยแพร่ข้อมูลคอมพิวเตอร์ลามก (มาตรา 14(4)) แห่งพระราชบัญญัติว่าด้วยการ

กระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 สามารถนำมาปรับใช้กับการตามรังควานบนอินเทอร์เน็ตได้ในระดับหนึ่ง

คำสำคัญ: อินเทอร์เน็ต การตามรังควานบนอินเทอร์เน็ต เว็บไซต์เครือข่ายสังคม ประมวลกฎหมายอาญา พ.ศ. 2499 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

Abstract

Cyberstalking is a form of harassment, which occurs in cyberspace. It inflicts psychological harm on its victims, ranging from anxiety, fears to suicidal thoughts. Due to the advent of social networking technology, cyberstalkers misuse the features of these technologies to harass their victims. Over the past few years, there have been reports of cyberstalking on social networking systems, not only in foreign countries but also in Thailand. This article aims to explore the nature of cyberstalking, which takes place on social networking sites, and also to analyze the existing criminal provisions under Thai law to see the extent to which these laws can be enforced against cyberstalking on social networking sites. The findings of the study reveal that the offences of coercion (Section 309), defamation (Sections 326 and 328), and intending to scare or frighten another person (Section 392) proscribed in the Thai Criminal Code 1956; and the offences of inputting false or forged data (Section 14(1)) into computers and disseminating obscene material via the Internet (Section 14(4)) proscribed in the Computer-Related Crime Act B.E. 2550, could be applied to cyberstalking to some extent.

Keywords: Internet, Cyberstalking, Social Networking Sites, Criminal Code B.E. 2499 (1956), Computer-Related Crime Act B.E. 2550 (2007)

Introduction

Cyberspace is virtual space created by the Internet – i.e. the network of computer networks at a global level. William Ford Gibson, an American novelist, coined the term 'cyberspace' in his short story *Burning Chrome* in 1982. However, it is Gibson's novel *Neuromancer* –published in 1984, which made the term 'cyberspace' well-known. (Shachtman, 2008). In cyberspace, people (Internet users) can contact and communicate with each other at any time and from almost all corners of the world, transcending temporal and spatial limitations of the physical world. Despite these positive features, the Internet has a dark side. It "may provide a threatening environment and expose individuals to great risks" (Barak and King, 2000: 517), since those with malicious intent may misuse it to harass other Internet users. Moreover, as the Internet allows Internet users to do online activities with a great degree of anonymity, it is increasingly difficult to identify an individual perpetrator of online harassment (Basu and Jones, 2007).

Cyberstalking is a form of harassment which occurs in cyberspace. It is noteworthy that the term 'cyberstalking' refers to cyber-harassment involving adults as perpetrators and victims. The similar term 'cyberbullying' denotes cyber-harassment perpetrated by young people towards young people. However, the terms are used interchangeably (The Times of India, 2001). Although the terminology may give an impression of a pernicious activity of the 'modern' era in which people's everyday life is connected in one way or another to information and communications technologies, it is not an entirely new phenomenon. As early as 1996 in the US it was reported that Cynthia Armistead and her five-year-old daughter were subjected to cyberstalking by a man named Richard Hillyard (Bocij, 2004: 16-17). Similarly, the media in the UK reported in 1999 that "Angela Westwater was stalked by a man who lived 5,000 miles away on another continent" ("Cyberstalking: Pursued in Cyber Space", 1999).

In my previous paper on cyberstalking published in 2005, I explored and discussed the legal responses to cyberstalking in the UK and the US (Pitaksantayothin, 2005: 57-61). Although there was no clear evidence at that time that cyberstalking occurred in Thailand, my 2005 paper aimed to bring potential harmful effects of cyberstalking to the attention of legal scholars, legislators and the relevant authorities in Thailand. Unlike the UK and the US, up to the present Thailand still does not have a law to deal specifically with cyberstalking. Therefore, I will examine the existing criminal law in Thailand to see which provisions can be applied to cyberstalking. In addition, whilst my previous paper focused on cyberstalking through email communications and Internet forums, due to the popularity of social media

over the recent few years the focal point of the present paper is cyberstalking on social networking sites.

In the first section, I will begin with a brief account on the nature of cyberstalking to give an overall picture of this form of cyber-harassment to readers (especially those who may not have had a chance to read my previous paper). Some updated information will be added. In the second section, I will give some recent examples of cyberstalking, which have occurred on social networking sites. In the final section, I will discuss how the relevant provisions of the Thai Criminal Code 1956 and the Computer-Related Crime Act 2007 can be enforced against cyberstalkers.

1. The Nature of Cyberstalking

To understand cyberstalking, it is necessary to begin the discussion with the question "What is cyberstalking?" There are many definitions of cyberstalking. In the Oxford Dictionary, cyberstalking is defined as "the repeated use of electronic communications to harass or frighten someone, for example by sending threatening emails". According to Paul Bocji, an expert in cyberstalking at Aston University, cyberstalking is a group of behaviors "in which an individual, group of individuals or organization uses information and communications technology to harass others" (Bocij, 2004: 14), and inflicting emotional distress on them. The Crown Prosecution Service (UK) defines cyberstalking as harassment that takes place on the Internet through the use of emails, chat rooms, social networking sites and other forums facilitated by information technology (The Crown Prosecution Service). It is important to note that for an online harassment to be classified as cyberstalking, the conduct has to continue for many weeks, months or years (Clough, 2010: 366). In other words, cyberstalking must be a course of conduct that lasts for a considerable period of time. Therefore, an online harassment that occurs only once or a few times may not be counted as cyberstalking. Most importantly, cyberstalking must have a psychological impact on victims, ranging from anxiety, sleep disturbances, post-traumatic stress disorder to suicidal thoughts (Clough, 2010: 366).

Cyberstalking comes in various forms, including "making threats, false accusations (false-victimization), abusing the victim, attacks on data and equipment, attempts to gather information about the victim, impersonating the victim [and sending abusive emails or fraudulent spams in the victim's name], (Ellison and Akdeniz, 1998) encouraging others to harass the victim, ordering goods and services on behalf of the victim, arranging to meet the victim and physical assault" (Chawki and el Shazly, 2013: 73). In some

cases, a cyberstalker may subscribe the victim's email address without permission to a number of mail lists, resulting in the victim receiving hundreds of unwanted emails (spams) everyday (Ellison and Akdeniz, 1998). The dissemination of sexually explicit photographs of the victim without permission on social networking sites can be considered as an instance of cyber-harassment. The perpetrator may post the victim's private photographs on a social networking site on a regular basis for a considerable period of time with the intention to inflict psychological harm (i.e. embarrassment) to the victim. Worse still, he would encourage others – especially those who know the victim personally – to harass the victim verbally or sexually, both in and outside of cyberspace. Therefore, it is reasonable to say that, in the broader sense, cyberstalking includes the posting of sexually explicit photographs of the victim without permission on social networking sites (Porterfield, 2011).

Bocij conducted a survey on cyberstalking by asking 169 respondents, both males and females, aged between 16 and 84 years old, living in the UK and the US to complete an online questionnaire. His survey published in 2003 reveals that "most cyberstalking victims were found to be female, aged 30 years or older and with a good level of education" (Bocij, 2003). Interestingly, "most respondents did not know the identity of the person who harassed them. Nonetheless, it is noteworthy that only a small number of respondents claimed to have been harassed by a friend (15.79%), a former partner (8.77%) or a work colleague (1.75%) (Bocij, 2003).

2. Incidents of Cyberstalking on Social Networking Sites

In the past, cyberstalking typically occurred through email communications and Internet forums – such as, web boards or bulletin boards and chat rooms (Pitaksantayothin, 2005: 55-56). However, since social networking sites have become an integral part of everyday life, it appears that cyberstalking also happens on social networking systems. A number of Internet users input and keep their private information (e.g. real names, addresses, telephone numbers, e-mail addresses, information about their families and photographs) on their social networking accounts. In most cases, they share such personal data with other social networking sites users, some of whom they barely know personally outside cyberspace. This allows cyberstalkers to search for and gather personal data of the victims with ease. In certain cases, cyberstalkers threaten the victims over the social networking systems. For instance, in 2011, Patricia Arquette – an American actress –was threatened by a stranger whom she had previously accepted as her 'facebook friend'. As a result, she decided to deactivate

her facebook account at the advice of her security team ("Arquette Shuts Down Facebook Account Over Stalker Fears", 2011).

Another form of cyberstalking on social media is cyber-impersonation. Some cyberstalkers gather personal information about their victims – such as names, addresses, phone numbers, email addresses and photographs – from the Internet (i.e. from search engines) and use such information to create imposter accounts on social networking sites. Subsequently, they use the imposter accounts to contact other social networking users and post messages which could impair the reputation of the victims. In 2013, a cyberstalker created a 'fake' account of Nilawan Panichrungrueng – a Thai news announcer, and posted several inappropriate messages on it, making other users misunderstand and think that it was she who posted such messages. Interestingly, Nilawan insisted that she did not have any social networking account ("ผู้ประกาศข่าวสาว 7 สี เต้นร้องกองปราบฯ ถูกมือมืดแอบอ้างในเฟซบุ๊ก", 2556).

In some cases, the cyberstalkers disseminate photographs of the victims engaging in sexual activities or being sexually abused via the social networking systems without the victims' permission. Tragically, some victims committed suicide as they could not endure the emotional distress caused by this form of cyberstalking, for example Rehtaeh Parsons, ("Canadian Teen Commits Suicide After Alleged Rape, Bullying", 2013) Amanda Todd ("Canadian Teen Found Dead Weeks After Posting Wrenching YouTube Video Detailing Bullying", 2012) and Audrie Pott ("I Swear To God If You Still Have Those Pics I'll Kill You', and The Pleading Facebook Messages Teen Sent Days Before She Killed Herself 'After Classmates Sexually Assaulted Her and Spread Images of Attack", 2013) are some examples of the victims of this heinous form of cyberstalking. Rehtaeh and Audrie were sexually abused while they were under the influence of alcohol. Their sexual abuse was recorded by cameras. Amanda was induced by a stranger to strip in front of the camera, which was set to record her naked body. The images of the three unfortunate girls being sexually abused were disseminated through social media, causing serious emotional pain and eventually leading to their suicides.

3. The Relevant Provisions of the Thai Criminal Code 1956 and the Computer-Related Crime Act 2007

As discussed above, there are mainly three types of cyberstalking on social networking sites: 1) threats on social networking sites 2) cyber-impersonation and 3) the dissemination of sexually explicit images of the victims against their wills on social networking

sites. Although Thailand does not have anti-cyberstalking legislation at the moment, some provisions in the Thai Criminal Code 1956 and the Computer-Related Crime Act 2007 could be – to a certain extent – applied to combat these three forms of cyberstalking.

Regarding the threats on social networking sites, the Computer-Related Crime Act 2007 – which regulates online activities – does not have a specific provision to criminalize the sending of threatening messages through social networking systems. However, the Thai Criminal Code 1956 does. In the case where a cyberstalker sends a threatening message to the victim, compelling him to do or not to do any act or putting him in fear of injury to his life, body, liberty, reputation or property or that of another person, he may be punished by Section 309. Furthermore, although the threat is intended merely to frighten or scare the victim, such an act is considered to be an offence under Section 392.

As far as cyber-impersonation is concerned, Section 14(1) of the Computer-Related Crime Act 2007 – which criminalizes the inputting of false or forged computer data, either in whole or in part, into a computer system which is likely to cause damage to others – could be enforced against this type of cyberstalking. This is because the use of an imposter account to make others misunderstand that the victim is the user of such account can be deemed as an act of inputting false or forged computer data into the Internet with an intention to damage the victim (especially his reputation).

The dissemination of sexually explicit images of the victim is punishable under certain provisions of the Computer-Related Crime Act 2007 and the Thai Criminal Code 1956. Section 14(4) of the Computer-Related Crime Act 2007 prohibits the inputting of obscene computer data into a computer system which is publicly accessible. It can be said that a cyberstalker who posts a sexually explicit picture of the victim on a social networking site is inputting obscene data into the Internet (which is a publicly accessible computer system). Thus, his act falls within the scope of Section 14(4). However, it should be noted that Section 14(4) is not designed to protect the victim from cyberstalking, as its main intention is to deal with obscene materials on the Internet, most of which are commercial items.

The dissemination of sexually explicit images may also be subjected to defamation law under the Thai Criminal Code 1956. Section 326 makes it an offence to '[impute] anything to the other person before a third person in a manner likely to impair the reputation of such other person or to expose such other person to be hated or scorned'. Section 328 imposes a criminal sanction on

a person who defames others 'by means of publication of a document, drawing, painting, cinematography film, picture or letters made visible by any means, gramophone record or other recording instruments, recording picture or letters, or by broadcasting or spreading pictures, or by propagation by any other means'. The dissemination of sexually explicit images of the victim via social media can be regarded as a form of defamation by means of publishing pictures and it seriously impairs the reputation of the victim. Therefore, a person who commits this form of cyberstalking may be charged with defamation.

It is interesting to note that a person who employs, coerces, threatens, hires or instigates another person to conduct cyberstalking is considered to be an instigator and thus can be punished as principal under Section 84 of the Thai Criminal Code 1956. Furthermore, a person who facilitates another person to cyber stalk is regarded as a supporter and can be punished under Section 86 of the Thai Criminal Code 1956. In addition, by virtue of Section 14(5) of the Computer-Related Crime Act 2550, a person who forwards sexually explicit pictures of the victim of cyberstalking is also subjected to criminal punishment.

Conclusion

As examined above, cyberstalking is a form of online harassment. It inflicts psychological harm on the victims in many ways, ranging from anxiety to suicidal thoughts. Some cyberstalkers misuse social networking sites to hunt down and harass their victims. There have been many reports about cyberstalking on social networking sites, both in Thailand and other countries. In Thailand, there may be cyberstalking incidents that are underreported or do not receive media attention. At present, Thailand does not have an anti-cyberstalking law like the UK and the US. However, as analyzed above, some of the existing criminal provisions prescribed in the Thai Criminal Code 1956 and the Computer-Related Crime Act 2007 could be applied to the three main forms of cyberstalking on social networking sites. However, it is doubtful whether this piecemeal legal measure can effectively prevent cyberstalking in Thailand. Given this, it is challenging to leave a final question here, namely whether Thailand should follow the UK and the US and have a specific anti-cyberstalking law or not. To know an answer, further research, especially from a criminological perspective, may be required.

References

"Arquette Shuts Down Facebook Account Over Stalker Fears" 2011, October 6. **USWeekly** [Online]. Available: http://www.usmagazine.com/celebrity-news/news/patricia-arquette-i-have-a-facebook-stalker-2011610

Barak, Azy, and King, Strom. 2000. "The Two Faces of the Internet: Introduction to the Special Issue on the Internet and Sexuality." **CyberPsychology and Behavior** 3, 4: 517-520.

Basu, Subhajit, and Jones, Richard. 2007 "Regulating Cyberstalking" **Journal of Information Law and Technology** [Online]. Available: http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2007__2/basu__jones

Bocij, Paul. 2003. "Victims of Cyberstalking: An Exploratory Study of Harassment Perpetrated via the Internet" **First Monday** [Online]. Available: http://firstmonday.org/ojs/index.php/fm/article/view/1086/1006

Bocij, Paul. 2004. **Cyberstalking : Harassment in the Internet Age and How to Protect Your Family**. Westport, C.T: Praeger Publishers.

"Canadian Teen Commits Suicide After Alleged Rape, Bullying" 2013, April 10. **CNN** [Online] Available: http://edition.cnn.com/2013/04/10/justice/canada-teen-suicide/index.html

"Canadian Teen Found Dead Weeks After Posting Wrenching YouTube Video Detailing Bullying" 2012, October 12. **Foxnews** [Online] Available: http://www.foxnews.com/world/2012/10/12/canadian-teen-found-dead-weeks-after-posting-wrenching-youtube-video-detailing/

"A Channel 7 News Anchor Reported to the Crime Suppression Division, Complaining that an Unknown Person Impersonated Her on Facebook" 2013, January 3. **Dailynews** [Online]. Available: http://www.dailynews.co.th/Content.do?contentId=136586 (in Thai).

"ผู้ประกาศข่าวสาว 7 สีเต้นร้องกองปราบฯถูกมือมืดแอบอ้างในเฟซบุ๊ก" 3 มกราคม 2556. **เดลินิวส์** [ออนไลน์]. เข้าถึงจาก: http://www.dailynews.co.th/Content.do?contentId=136586

Chawki, Mohamed, and el Shazly, Yassin. 2013. "Online Sexual Harassment: Issues & Solutions" **Journal of Intellectual Property, Information Technology and E-Commerce Law** Vol. 4: 71-86.

Clough, Jonathan. 2010. **Principles of Cybercrime**. Cambridge: Cambridge University Press.

The Crown Prosecution Service **Stalking and Harassment** [Online]. Avialable: http://www.cps.gov.uk/legal/s__to__u/stalking__and__harassment/

"Cyberstalking: Pursued in Cyber Space" 1999, June 26. **BBC** [Online]. Available: http://news.bbc.co.uk/2/hi/uk__news/

378373.stm.

Cyberstalking [Online]. Available: http://www.oxforddictionaries.com/definition/english/cyberstalking?q=cyberstalking

Ellison, Louise, and Akdeniz, Yaman. 1998. "Cyber-stalking: The Regulation of Harassment on the Internet" **Criminal Law Review,** Special Edition: Crime, Criminal Justice and the Internet, [Online]. Available: http://www.cyber-rights.org/documents/stalking__article.pdf

"'I Swear To God If You Still Have Those Pics I'll Kill You': The Pleading Facebook Messages Teen Sent Days Before She Killed Herself 'After Classmates Sexually Assaulted Her and Spread Images of Attack'" 2013, September 18. **Mail Online** [Online] Available: http://www.dailymail.co.uk/news/article-2424412/Audrie-Pott-death-Facebook-messages-sent-teen-days-killed-herself.html

Pitaksantayothin, Jompon. 2005. "Cyberstalking : Criminal Offences in the US and the UK." **Burapha University Journal of Humanities and Social Science** 13, 19: 51-65 (in Thai).

จอมพล พิทักษ์สันตโยธิน. 2548. "การตามรังควานบนอินเทอร์เน็ต กับความผิดทางอาญาในสหรัฐอเมริกาและสหราชอาณาจักร" **วารสารวิชาการมนุษยศาสตร์และสังคมศาสตร์** 13, 19: 51-56.

Porterfield, Elaine. 2011. "Preteen Girls Charged with Cyberstalking near Seattle" **Reuters** [Online]. Available: http://www.reuters.com/article/2011/04/26/us-cyberstalking-girls-idUSTRE73P7CV20110426

Shachtman, Noah. 2008. "26 Years After Gibson, Pentagon Defines 'Cyberspace'." **Wired** [Online]. Available: http://www.wired.com/dangerroom/2008/05/pentagon-define/

The Times of India. 2011. **Cyber Stalking** [Online]. Available: http://articles.timesofindia.indiatimes.com/2011-06-06/personal-tech/29722217__1__cyber-stalking-stalkers-chat

Dr. Jompon Pitaksantayothin graduated from Thammasat University with an LL.B. (2nd Class Honors); from the University of Warwick with an LL.M. in International Economic Law (with Merit); from the University of Edinburgh with an LL.M. and from the University of Leeds with a Ph.D. in Cyber Law. He also received a certificate in the Korean Language from Korea University. At present he works as a full-time lecturer in School of Law, University of the Thai Chamber of Commerce.